AFFIDAVIT OF J. CHRISTOPHER WOOD IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, J. Christopher Wood, being first duly sworn, hereby depose and state as follows:

A. Introduction and Agent Background

1. I am a Senior Special Agent with the U.S. Department of the Interior (DOI), Office of Inspector General (OIG), Office of Investigations assigned to the central region field office in Billings, MT. I have been employed by DOI/OIG since October 1998. I have over 16 years of law enforcement experience. During my 13 years as a federal criminal investigator, I have conducted numerous criminal investigations, including those involving public corruption; contract and grant fraud; child pornography; theft or embezzlement cases by government employees and those who do business with the federal government; and other serious instances of misconduct by federal employees. Often, particularly in the last 10 – 15 years, such crimes have involved use of the Internet. I hold a Bachelor of Science Degree in General Business from Miami University in Oxford, Ohio. I am a Certified Fraud Examiner. My formal training includes the successful completion of the Criminal Investigator Training Program, the Digital Evidence Acquisition Specialist Training Program, the Grant Fraud Investigations Training Program, and the Continuing Legal Education Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also attended training seminars on Search and Seizure Law, Public Corruption Investigations, and Money Laundering Investigations sponsored by the U.S. Attorney's Office in conjunction with the Federal Bureau of Investigation and the Internal Revenue Service.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation (hereafter referred to as Microsoft), a provider of electronic mail (e-mail), instant messaging, and related Internet services, headquartered at One Microsoft Way, Redmond, Washington 98052 and whose custodian of records is located at 1065 La Avenida, Building #4, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to require Microsoft to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the referenced accounts, including the contents of communications.

3. The facts set forth in this affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. Through my experience and training I am aware that perpetrators of financial fraud schemes, including fraudulent investment schemes, utilize e-mail to communicate with past and current victims of their schemes. The perpetrators of these financial fraud schemes also utilize e-mail to promote their schemes in an effort to entice and attract new victims to the scheme.

B. Applicable Law

5. Title 18, United States Code, Section 1341 makes it a Federal crime for any person who:

> having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both.

6. Title 18, United States Code, Section 1343 makes it a Federal crime for any person who:

> having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

C. Background Information - The Internet and IP Addresses

7. The Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state. This connectivity allows data to be stored and exchanged

between computers remotely. Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers (ISPs).

8. An Internet Service Provider (ISP) is a business that provides access to the Internet and the World Wide Web. Services provided by an ISP include computer accounts, Internet access and connection to the Internet via a telephone line and a modem. Given the interstate and international nature of the Internet, all ISP computers that are connected to the Internet are used in interstate or foreign commerce or communication.

9. ISPs offer their customers access to the Internet through computer systems they administer and typically offer a variety of services, including electronic mail (e-mail), data storage and on-line chat rooms.

10. ISP customers often use a home computer, which communicates through a modem over a telephone line, to access an ISP's computer system. Often, a customer accesses the ISP's computer system by using a username and password. The username is typically a nickname or other pseudonym chosen by the user.

11. Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. Other addresses include Uniform Resource Locator (URL) addresses, such as "http://www.usdoj.gov," which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use.

12. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

13. Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users. User names and IDs are typically associated with additional user information or resources, such as a user account protected by a password, personal or financial information about the user, a directory of files, or an e-mail address.

14. Communication between two or more computers can occur in many ways. Two of the most common ways are via e-mail and on-line chat. E-mail, short for electronic mail, is primarily text messages sent between two or more computers. An

on-line chat is a casual conversation wherein two or more individuals connected to the Internet have real-time text-based conversations by typing messages into their computers.

15. Instant Messaging (IM) is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state.

D. Statement of Probable Cause

16. The following information is based on my own personal investigation.

17. On October 20, 2006, the U.S. Department of the Interior, Bureau of Indian Affairs (hereafter referred to as BIA), Ft Peck Agency, 500 Medicine Bear Road, Poplar, Montana 59255, approved Oil and Gas Lease Numbers 14-20-0256-0388, 14-20-0256-0389, and 14-20-0256-0390 on the Ft Peck Indian Reservation for Domestic Energy Solutions, 5818 Via Romero, Yorba Linda, California 92887.

18. Some of the known representatives of Domestic Energy Solutions are Suzette Gal and Michael Hertel.

19. On October 17, 2007, the BIA sent a letter to Domestic Energy Solutions via certified mail informing Domestic Energy Solutions that Oil and Gas Lease Numbers 14-20-0256-0388, 14-20-0256-0389, and 14-20-0256-0390 on the Ft Peck Indian Reservation were cancelled effective October 5, 2007 due to Domestic Energy Solutions non-payment of past due fees, rental amounts, and bonus amounts.

20. The October 17, 2007 letter from the BIA was delivered to and signed for by Suzette Gal, Domestic Energy Solutions, on October 27, 2007.

21. On October 27, 2007, Domestic Energy Solutions became aware that their oil and gas leases on the Ft Peck Indian Reservation were cancelled. Since that date, neither Michael Hertel, nor Suzette Gal, nor Steve Carpenter, nor Myron White, nor Domestic Energy Solutions, nor U.S. Energy, nor U.S. Oil and Gas, LLC have applied for any oil and gas leases on the Ft Peck

Indian Reservation. None of these individuals or companies have any approved oil and gas leases on the Ft Peck Indian Reservation.

22. In July 2010, the BIA was contacted by Mervin L. Ezray, 7 Park Sierra Lane, Sacramento, California 95864, concerning investments Ezray had made with Domestic Energy Solutions. Ezray told the BIA that he had invested over $37,000 with Domestic Energy Solutions based upon a copy of the October 20, 2006 letter from the BIA to Domestic Energy Solutions informing the company that Oil and Gas Lease Numbers 14-20-0256-0388, 14-20-0256-0389, and 14-20-0256-0390 on the Ft Peck Indian Reservation had been approved. Ezray told the BIA that he dealt with Michael (Mike) Hertel from Domestic Energy Solutions and that the company's e-mail address was domesticenergy@att.net. Ezray told the BIA that he had not received any returns on his investment with Domestic Energy Solutions, despite Hertel's statements to him that he would receive payment. Ezray told the BIA that he was no longer able to make contact with Hertel or Domestic Energy Solutions.

23. In his July 16, 2010 letter to the BIA, Mervin L. Ezray stated that when Domestic Energy Solutions provided him with a copy of the October 20, 2006 letter from the BIA which stated the three oil and gas leases on the Ft Peck Indian Reservation had been approved for Domestic Energy Solutions, that this gave him confidence to invest with the company.

24. On October 13, 2010, the BIA was contacted by Wanda Cagliari, 3700 Boyer Road, Fallon, Nevada 89406, concerning investments Cagliari had made with Domestic Energy Solutions. Cagliari told the BIA that she had invested $2,500 with Domestic Energy Solutions. Cagliari provided the BIA with a copy of the October 20, 2006 lease approval letter that she received from Domestic Energy Solutions. Cagliari also provided the BIA with a copy of a letter dated October 8, 2010 from Mike Hertel, Domestic Energy Solutions to Cagliari. The October 8, 2010 letter informed Cagliari that her $2,500 investment with Domestic Energy Solutions entitled her to a ¼% ($3,125 retail) ownership in Domestic Energy Solutions and all income generated, which includes but is not limited to the following leases on the Ft Peck Indian Reservation, 14-20-0256-0388, 14-20-0256-0389, and 14-20-0256-0390. The October 8, 2010 letter also informed Cagliari that her ¼% ownership would include income generated by Domestic Energy Solutions currently operating drilling rig and future income from a refinery, pipelines, and other land leases. The October 8, 2010 letter informed Cagliari that she would recoup her initial investment within 30 days and would receive monthly checks thereafter of approximately 4-5% of $3,125. The letter also informed Cagliari that she would receive in excess of $700 per month from the refinery beginning within 6-8 months and that she would earn approximately $1.25 per barrel of oil produced on all wells. The October 8, 2010 letter provided to the BIA by Cagliari indicated that Domestic Energy Solutions company e-mail address was domesticenergy@hotmail.com.

25. Domestic Energy Solutions has never had an operating drilling rig on the Ft Peck Indian Reservation as they claimed in their letter to Wanda Cagliari.

26. On April 15, 2011, the BIA was contacted by Rawland Strang, 95 Oroview Drive, Oroville, California 95965, concerning investments Strang had made with Domestic Energy Solutions. Strang provided the BIA with a copy of a letter dated March 7, 2011 from Mike Hertel, Domestic Energy Solutions to Strang. The March 7, 2011 letter informed Strang that his $4,000 investment with Domestic Energy Solutions entitled him to a 1/2% ownership in Domestic Energy Solutions and all income generated, which includes but is not limited to the following leases on the Ft Peck Indian Reservation, 14-20-0256-0388, 14-20-0256-0389, and 14-20-0256-0390. The March 7, 2011 letter also informed Strang that his ½% ownership would include income generated by Domestic Energy Solutions currently operating drilling rig and future income from a refinery, pipelines, and other land leases. The March 7, 2011 letter informed Strang that he would recoup his initial investment by the end of April 2011 and would receive monthly checks thereafter of approximately 4-5%. The letter also informed Strang that he would receive income in excess of $750 from the refinery and that he would earn approximately $0.90 per barrel of oil.

27. Domestic Energy Solutions has never had an operating drilling rig on the Ft Peck Indian Reservation as they claimed in their letter to Rawland Strang.

28. Lisa Boxer, Realty Specialist, BIA, Ft Peck Agency, said she spoke with Rawland Strang in April 2011 and told him that Domestic Energy Solutions did not have any approved oil and gas leases on the Ft Peck Indian Reservation.

29. On June 28, 2011 at 1:50 p.m., Michael Hertel sent an e-mail to the BIA with a subject line of letter of intent. The body of the e-mail read, "Attached is a rough draft of a letter of intent. Will this be sufficient?" Attached to the e-mail message from Hertel was a Letter of Intent for Business Transactions dated June 28, 2011. The draft letter of intent was a proposal between U.S. Energy, 18340 Yorba Linda Boulevard #153, Yorba Linda, California 92887 and the Ft Peck Indian Reservation to allow U.S. Energy to drill for and produce crude oil and to install a 20,000 barrels per day oil refinery on the Ft Peck Indian Reservation. The signature block on the letter of intent for U.S. Energy listed Myron White as its partner. The e-mail message was sent from the e-mail address goldnugget13@att.net.

30. On June 28, 2011 at 1:52 p.m., Michael Hertel sent an e-mail to the BIA with a subject line of re: letter. The body of the e-mail read, "our number is 213 928 5750 steve or mike" The e-mail message was sent from the e-mail address goldnugget13@att.net.

31. On October 18, 2011, Myron White, US Oil and Gas, LLC, contacted the BIA and requested the BIA sign a Letter of Intent to allow US Oil and Gas, LLC to build an oil refinery on the Ft Peck Indian Reservation.

32. On October 18, 2011, approximately ten minutes after Myron White had contacted the BIA, Steve Carpenter, US Oil and Gas, LLC contacted the BIA and also requested the BIA sign the Letter of Intent.

33. On October 5, 2011, U.S. Oil and Gas, LLC, 300 Smelter Avenue #179, Great Falls, Montana 59404 mailed to the BIA via U.S. Postal Service Priority Mail flat rate mailing envelope the following documents:

1) U.S. Department of the Interior, BIA, Evidence of Authority of Officers to Execute Papers form dated October 4, 2011. The notarized form stated that Steve Carpenter was the President of U.S. Oil and Gas, LLC and that Myron White was the Secretary of U.S. Oil and Gas, LLC. The form stated U.S. Oil and Gas, LLC was a corporation organized under the laws of Montana. Myron White signed the form and listed his title as Managing Partner.

2) A letter dated July 13, 2011, from Linda McCulloch, Secretary of State, State of Montana, stating the Articles of Organization for U.S. Oil and Gas, LLC had been approved.

3) Articles of Organization filing application for U.S. Oil and Gas, LLC dated July 11, 2011.

4) A Letter of Intent for Business Transactions dated October 4, 2011. The Letter of Intent was a proposal between U.S. Oil and Gas, LLC, 300 Smelter Avenue #179, Great Falls, Montana 59404 and the Ft Peck Indian Reservation to allow U.S. Oil and Gas, LLC drill for and produce crude oil and to install a 20,000 barrels per day oil refinery on the Ft Peck Indian Reservation. The Letter of Intent was signed on behalf of U.S. Oil and Gas, LLC by Myron White.

34. The October 5, 2011 mailing from U.S. Oil and Gas, LLC, 300 Smelter Avenue #179, Great Falls, Montana 59404 was postmarked from Anaheim, California 92809. The BIA received the mailing on October 11, 2011.

35. On October 21, 2011, Steve Carpenter, U.S. Oil and Gas, LLC, contacted the BIA again and requested the BIA e-mail him a letter stating that the BIA had received U.S. Oil and Gas, LLC's Articles of Organization, the Evidence of Authority of Officers to Execute Powers document, and the Letter of Intent for Business Transactions. Carpenter provided the company e-mail address as usoil@att.net.

36. On October 26, 2011, Steve Carpenter again contacted the BIA requesting a letter stating that the BIA had received U.S. Oil and Gas, LLC's Articles of Organization, the Evidence of Authority of Officers to Execute Powers document, and the Letter of Intent for Business Transactions.

37. On November 16, 2011, Arthur S. Bahler, 207 South 10th Street, Fairbury, Illinois 61739, contacted the BIA concerning an investment opportunity with U.S. Oil and Gas, LLC. Bahler told the BIA that he had spoken with Steve Carpenter, U.S. Oil and Gas, LLC and that he (Bahler) was considering investing money with the company. Bahler said he was contacting

the BIA to confirm that U.S. Oil and Gas, LLC did in fact have oil and gas leases on the Ft Peck Indian Reservation. The BIA informed Bahler that U.S. Oil and Gas, LLC did not have any oil and gas leases on the Ft Peck Indian Reservation.

38. None of the currently identified victims (Ezray, Cagliari, and Strang) have been contacted by law enforcement officials for fear that contacting them at this point in time could jeopardize potential proactive investigative efforts in this case.

39. Hotmail is an internet e-mail service provided by Microsoft. Hotmail is a registered trademark of the Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052.

40. The Microsoft Online Services Global Criminal Compliance Handbook states on Page 5 under the heading E-Mail Services, subheading What are the Various E-mail Services Microsoft Provides?, that one of the many domains owned and operated by Microsoft are the @hotmail.com domain addresses.

41. The Microsoft Online Services Global Criminal Compliance Handbook states on Page 3 under the heading Where to Serve Legal Process in Criminal Matters? that legal process for online services should be provided to Microsoft Corporation, ATTN: Online Services Custodian of Records, One Microsoft Way, Redmond, Washington 98052. This section of the handbook lists the fax number for legal compliance as (425) 708-0096 and the Law Enforcement Hotline number as (425) 722-1299.

42. When I called the Microsoft Law Enforcement Hotline number (425-722-1299), the recorded message from Microsoft stated that the physical location for Microsoft's Online Services Custodian of Records was 1065 La Avenida, Building #4, Mountain View, California 94043. The recorded message stated the fax number for legal process for online services was (425) 708-0096.

E. Relevant Electronic and Wire Communication Statutes

43. The relevant federal statutes involved in the disclosure of customer communication records are as follows:

a. 18 U.S.C. § 2703(a) provides, in part: "A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."

b. 18 U.S.C. § 2703(b)(1)(A) provides, in part: "A governmental entity may require a provider of remote computing service to disclose the contents of a wire or electronic communication . . . (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."

c. 18 U.S.C. § 2703(c)(1)(A) provides, in part: "A governmental entity may require a provider of electronic communication service or remote computing to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity — (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."

d. 18 U.S.C § 2510(1) defines a "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications affecting interstate or foreign commerce."

e. 18 U.S.C. § 2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with certain exceptions not applicable here.

f. 18 U.S.C § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

F. Technical Background

44. E-mail is an electronic form of communication which usually contains written correspondence and graphic images. It is similar to conventional paper mail in that it is addressed from one individual to another and is usually considered private. An e-mail usually contains a message "header" which generally displays the sender's e-mail address, the recipient's e-mail address, and the date and time of the e-mail transmission.

45. If a sender chooses to do so, he or she can type a subject line into the header. E-mail message "headers" usually contain information, such as identification of the sender's ISP, which enables law enforcement officers to trace the message back to the original sender. In order to do so, information must be obtained from the sender's ISP through a Grand Jury or administrative subpoena.

46. Microsoft is, among other things, a U.S.-based Internet Service Provider or "Web Hosts." Microsoft provides a full range of services including but not limited to: web based e-mail accounts, search engines, directories, travel resources, commercial services, and advertising. Microsoft provides individuals with free web based e-mail accounts and Instant Messaging services.

47. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including e-mail access, to the general public. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft's subscribers) and information concerning subscribers and their use of Microsoft's services, such as account access information, e-mail transaction information, and account application information.

48. In general, an e-mail that is sent to Microsoft's subscribers is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely.

49. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Microsoft's servers, the e-mail can remain on the system indefinitely.

50. Microsoft's subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Microsoft.

51. Subscribers to Microsoft might not store on their home computers copies of the e-mails stored in their account. This is particularly true when they access their account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

52. In general, e-mail providers like these companies ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

53. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e. session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Microsoft's websites), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

54. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

55. In my training and experience, I have learned that evidence of who was using an e-mail account and Instant Messenger accounts may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

G. Procedure for Search and Seizure

56. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B.

Upon receipt of the information described in Attachment B, the case agents (or other government-authorized personnel) will review all of the information. During the case agents' review of the information, the agents will segregate the information into two groups: (i) information that is the target of the warrant listed in Attachment B and which the government may therefore seize; and (ii) information that is not the target of the warrant.

Government personnel will "seize" information that is the target of the warrant listed in Attachment B by copying it onto a separate storage device or medium. Such information may be used by law enforcement in the same manner as any other seized evidence.

Information that is not the target of the warrant will be sealed in a secure location. Such information will not be reviewed again without further order of the court (e.g., subsequent search warrant, or order to unseal by the district court).

H. Conclusion

57. Based on my training and experience, and the facts as set forth in this affidavit, I have probable cause to believe that on Microsoft's computer servers there exists evidence of violations of the above-described criminal statutes. Accordingly, a search warrant is requested.

58. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

59. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

/s/ J. Christopher Wood

J. Christopher Wood
Special Agent
Department of the Interior
Office of the Inspector General

Subscribed and sworn to before me this 16th day of December 2011.

The Honorable Keith Strong
United States Magistrate Judge